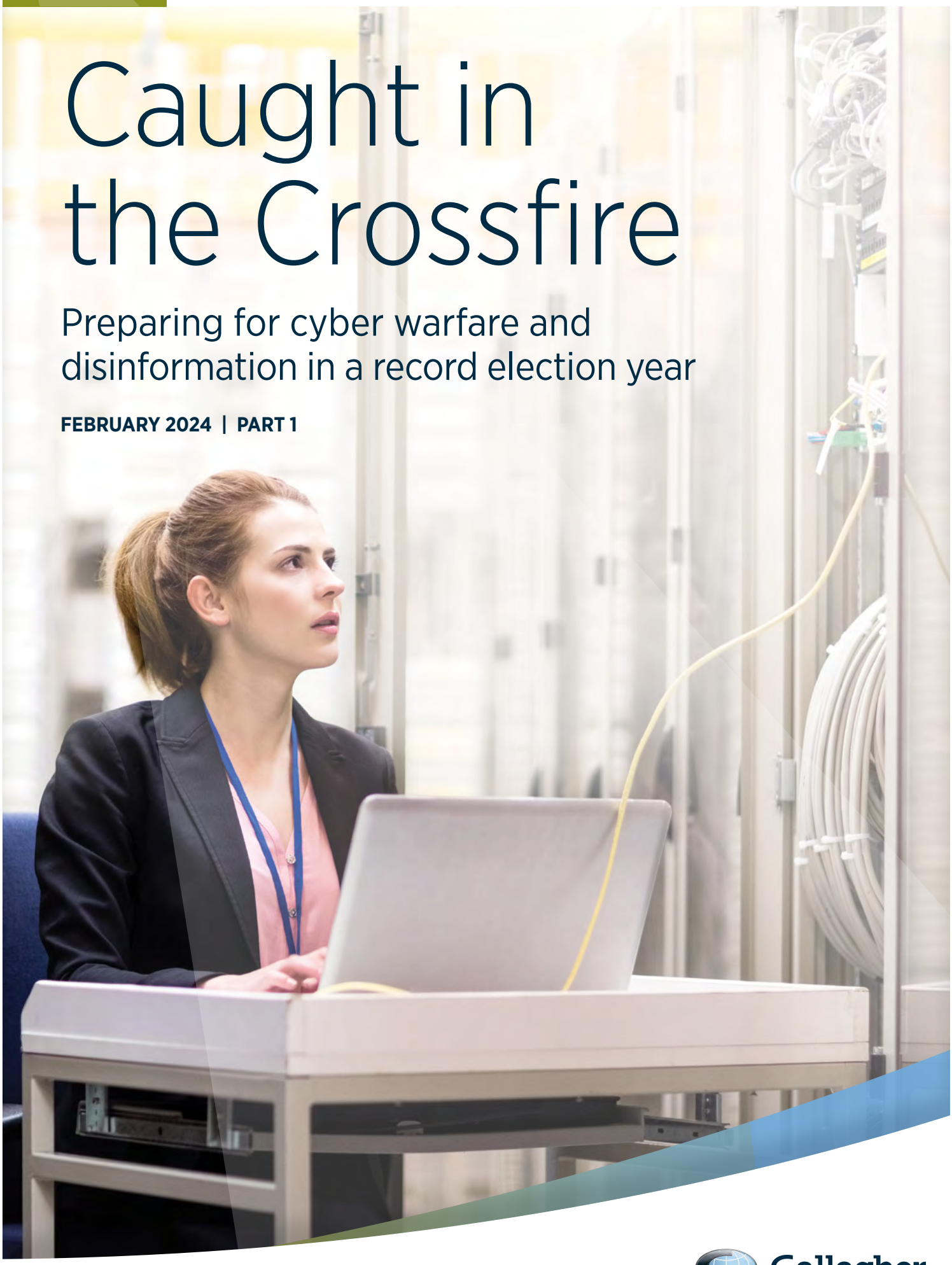
Spotlight

SHIFTING PERSPECTIVES

Caught in the Crossfire

Preparing for cyber warfare and disinformation in a record election year

FEBRUARY 2024 | PART 1



Gallagher

Key findings

1. National elections are taking place in at least 64 countries in 2024 and **AI-fueled disinformation campaigns are ramping up**.
2. Over time, **disinformation erodes trust in public institutions** and affects how both the public and private sectors are perceived and governed.
3. Against a backdrop of increasingly unstable geopolitics and global conflicts, **the frequency and severity of cyber warfare is expected to grow**.
4. **Businesses could be exposed to spillover attacks from state-sponsored intrusions** and to malware targeting software supply chains.
5. **Cyber insurance buyers should stress-test** how their policies are likely to respond in the event of a spillover attack.

2024: A year of elections in an unstable world

National elections are taking place in over 80 countries around the world in 2024, including elections in the US, Mexico, South Africa, Ukraine, Indonesia, Taiwan, the UK, Pakistan, and India. Against a backdrop of increasingly unstable geopolitics and global conflicts, the frequency and severity of cyber warfare and disinformation campaigns are expected to grow, in large part with the aim of tampering with the democratic process.[1]

While state-sponsored intrusions are generally aimed at governments and critical infrastructure, the risk of spillover attacks remains an ongoing business concern. Meanwhile, there are significant implications associated with the ability of artificial intelligence (AI) to create and spread misinformation at a scale and speed hitherto not seen.

"This year is the largest election year in history," says Jake Hernandez, CEO at AnotherDay, a Gallagher company specializing in crisis and intelligence consultancy. "There are over two billion people expected to be going to the polls. And the problem with that, especially now we've had this quantum leap in AI, is that technology to sow disinformation and distrust at nation-state scales is now available to pretty much anyone."

"Whereas in 2016, you had troll farms like the Internet Research Agency in St. Petersburg, you don't even need those anymore. Because you can get AI to be the trolls. So the potential is absolutely there for it to be a lot worse if there are not very proactive measures to deal with it. I don't think governments have really woken up to the risk at all."

"AI allows you to personalize messages and influence potential voters at scale, and that further erodes trust and has the potential to really undermine the functioning of democracy, which is really very dangerous," says Hernandez.

According to this year's World Economic Forum Global Risks Report, "The growing concern about misinformation and disinformation is in large part driven by the potential for AI, in the hands of bad actors, to flood global information systems with false narratives." [2]

"AI allows you to personalize messages and influence potential voters at scale, and that further erodes trust and has the potential to really undermine the functioning of democracy, which is really very dangerous."

— Jake Hernandez, CEO, AnotherDay

AnotherDay, a Gallagher Company is a specialist consultancy firm working with insurers on strategic risk advisory encompassing cyber threats, geopolitical intricacies, and climate change implications. The AnotherDay team works in conjunction with Gallagher's core insurance broking businesses as a complementary risk management and consulting service for clients.

Erosion of trust as disinformation spreads

There are a number of ways in which the spread of misinformation and disinformation can impact business risks. The prospect of election outcomes being influenced by propaganda wars undermines the democratic process with a polarizing impact.[3]

Over time, disinformation erodes trust in public institutions and affects how both the public and private sectors are perceived and governed. There are potential regulatory outcomes, with populist governments tending toward more light-touch regulatory regimes, for instance, yet at the same time often causing profound disruption within the corporate landscape.[4]

"The 2016 elections was the first real instance where we saw a misinformation/disinformation campaign being used," adds Laura Hawkes, head of Intelligence, AnotherDay. "Now that it's been tried and tested, and the tools have been sharpened for certain sorts of players, it's likely we'll see it again. Regulation of tech firms is going to be essential."

"From a business perspective and from the perspective of the general public, it means the world is a lot more uncertain," she continues. "The advent of AI is going to impact at least some elections. AI means that content can be made cheaper and produced on a mass scale. As a result, the public and also companies, are going to lose trust in what's being put out there."

Research by Yale University found that the ability to make educated decisions is eroded as a result of disinformation campaigns. Even at a senior level, the manipulation of behaviors (evident during the rollout of COVID vaccines, for example) and rising distrust of expert input lead to indecision, bias, and the potential for reputational consequences.[5]

According to this year's Edelman Trust Barometer, fear of an information war has risen substantially year on year. The report reveals an increase in the belief that societal leaders, including journalists, government leaders, and business leaders are purposely trying to mislead people by saying things they know are false.[6]

"Against the backdrop of the biggest global election year in history with more than 50 elections slated to take place, trust is under siege from a number of forces," said Kirsty Graham, president, Global Practices and Sectors at Edelman in a statement. "Concern over the impacts of innovation and those driving it have led to greater suspicion of economic and political systems. Institutions must work together to help address these concerns to allow a pathway for continued innovation and progress."

"The 2016 elections was the first real instance where we saw a misinformation/disinformation campaign being used. Now that it's been tried and tested, and the tools have been sharpened for certain sorts of players, it's likely we'll see it again. Regulation of tech firms is going to be essential."

— Laura Hawkes, Head of Intelligence, AnotherDay

The digital battleground heats up

In the past year, major cyber incidents have touched 120 countries, with targeted attacks fueled by government-sponsored actors also rising. Nearly half of these attacks targeted NATO member states, and more than 40%[7] were leveled against government or private-sector organizations involved in building and maintaining critical infrastructure.[8]

While headline-grabbing attacks during the past year were often focused on ransomware and perpetrated by organized criminal gangs, the MO is starting to change. Increasingly, according to cybersecurity commentator Daniel Lohrmann, "the predominant motivation has swung back to a desire to steal information, covertly monitor communication, or manipulate what people read."[9]

In February 2023, Iranian digital spies launched an attack on several Middle Eastern organizations using malware to target email accounts. The group responsible was allegedly linked to the Iranian intelligence services.[10] The following month, pro-Russian cyberthreat actors carried out a distributed denial-of-service (DDoS) attack on the French Senate's website, disrupting the services for several hours,[11] citing France's support for Ukraine as a motive.

There were numerous other politically motivated attacks during 2023.[12] Increasingly turbulent geopolitics have given rise to targeted cyber attacks on government and public agencies. In December 2023, the UK and its allies exposed a series of attempts by the Russian Intelligence Services (FSB) to target high-profile individuals and government entities with the aim of "interfering in politics and democratic processes."

In a statement to Parliament, the UK's Minister for Europe Leo Docherty said the government had "uncovered numerous instances of Russian intelligence targeting of critical national infrastructure" and that it had "worked in close co-ordination with our intelligence partners to expose sophisticated cyber-espionage tools aimed at sensitive targets."

Caught in the cyber crossfire

State-sponsored cyber attacks are becoming more targeted in nature, but at the same time are growing in frequency (with the proportion of nation-funded cyber attacks jumping from 20% to 40% in the past two years).[13] Moreover, state-sponsored actors are typically well funded and have highly specialist skills.

The risk of spillover remains a critical issue for businesses around the world. Some of the most disruptive cyber attacks to date — including the 2017 NotPetya ransomware attack — were carried out by politically motivated state actors.[14]

Businesses should be cognizant of the threat of spillover attacks, according to John Farley, managing director, Cyber Liability practice, Gallagher in the US.[15] "We are seeing a deliberate attempt to attack key players in the supply chain, such as software providers," he explains. "Once successfully attacked, threat actors can gain access to all of the software provider's client's data. I am not sure if elections will be the primary motivating factor," he continues. "Rather, geopolitical tensions overall."

According to WEF Global Risks, cyber attacks rank fifth globally in the current risk landscape, with attacks on critical infrastructure ranking in ninth place. "State-backed campaigns could deteriorate interstate relations... [and lead to] cyber offense operations with related spillover risks," it notes.[16]

Meanwhile, cyber attacks on power grids[17] and transportation systems,[18] for instance, can cause significant disruption to day-to-day business activities, while attacks on healthcare systems puts people directly at risk, State-sponsored cyber intrusions are becoming more sophisticated, targeted, and costly every year. Certain sectors have proved particularly vulnerable, such as the healthcare sector, which recorded a 74% spike in cyber attacks in 2022 compared to 2021.[19]

The US Department of Homeland Security (DHS) anticipates cyber espionage to be one of the most significant threats to the federal and local government establishments for 2024.[20] It predicts more state-funded attacks, and the increased spread of disinformation and misinformation.[21] The DHS also points to learnings from the 2016 election period[22] as having bolstered preparedness as the US progresses toward its November 5 election date.

NotPetya — how a suspected state-sponsored cyber attack became systemic and reshaped the cyber insurance market

According to Gallagher Re's Gray Rhino series, NotPetya was one of the most destructive pieces of code from the last decade.[23] The ransomware attack is also the closest the world has come to a systemic cyber event or cyber catastrophe.

Released in 2017 to primarily target Ukrainian firms and believed to have been backed by Russia, it took advantage of a vulnerability in Windows software. The malware went viral, causing economic damage of over $10 billion and impacting thousands of organizations — including many high-profile multinationals — in over 60 countries.

The attack changed how insurance carriers thought about and prepared for systemic cyber risk. Today, most policies include exclusions for cyber warfare and systemic-type events, although most wordings have yet to be properly tested in the courts.

Security frameworks tighten in anticipation

The activities of state-sponsored threat actors have triggered heightened cybersecurity awareness, threat intelligence, international cooperation, and the development of defensive measures to counter future threats. In particular, public-private operational collaboration heralds a new era of cyber resilience, with generative AI proving to be a new tool in the armory.[24]

Amid shifting geopolitics and "democracy's Super Bowl"[25] year of elections, governments across the world are revising their cybersecurity policies. The EU and NATO, for instance, have stepped up their cooperation with the launch of a task force focused on protecting energy, transport, digital infrastructure, and space from cyber espionage.[26]

There have been notable successes to date, including the international "Cookie Monster" sting, which took down the largest illicit cybercrime forum known as Genesis Market; and more recently the Five Eyes takedown of the Snake malware and data theft network used in espionage campaigns by Russia's Federal Security Service.[27]

Cyber risk management best practice

For organizations, the first step to employing a robust cyber protection system is to identify threats, the motive behind the attack and the threat direction. Identifying the hacker's technique is essential in forming the best line of defense, which should comprise technology and employee awareness.

Research and development in the field of cybersecurity has seen the introduction of new security automation platforms and technologies that can continually monitor systems to detect vulnerabilities and send notifications in case of detected malicious activities. Penetration testing is among the available services, which increasingly leverages the power of generative AI to improve the ability to detect suspicious anomalies.[28]

Robust data security policies and systems may often struggle to overcome human vulnerabilities. This is why organizations are increasingly investing in employee education and cybersecurity awareness in an effort to thwart cyberthreats.[29]

Cybersecurity teams are leaning toward security methods such as zero trust, network segmentation, and network virtualization to remove the risk of human error.[30] Zero trust security works on the principle of never trust, always verify — requiring identity and device verification at every attempt.[31]

Scenario plan for spillover threats

While a relatively remote threat, the potential for systemic spillover attacks is a concern that CISOs, risk professionals, and other cybersecurity personnel should be planning for. Supply chain attacks and major ransomware events over the past decade have shown how quickly disruption can spread across networks and businesses, with no regard for international borders.

Beyond maintaining effective cybersecurity protocols, businesses should have a tried and tested event response plan. This should include dedicated teams of IT forensic, legal, and crisis management experts, along with contingency plans to help contain any fallout and minimize the extent of network interruption and business downtime if and when the worst happens.

Businesses should sit down with their brokers and other advisors to stress-test how cyber insurance policies might respond if their firm is caught in the crossfire of a state-sponsored attack. "Most carriers are expanding the scope of the exclusion around war and imposing sublimits around other systemic events," says John Farley.

"We are advising our clients to pay particular attention around wording specific to attribution, level of harm in a claim scenario, whether war is formally declared or not, and wording that may impact coverage for parties not directly involved in a particular conflict or those impacted by the cascading effects of an attack on another party."

> "We are advising clients to pay particular attention around wording specific to attribution… [such as] whether war is formally declared or not, and wording that may impact coverage for parties not directly involved in a particular conflict."
>
> ***— John Farley, Managing Director, Cyber Liability Practice, Gallagher***

Citations

1 "Global Risk Forecast 2024," CRISIS24, Jan. 2024

2 "Global Risks Report 2024," World Economic Forum, 10 Jan. 2024

3 Reglitz, Merten. "'Fake news' poses corrosive existential threat to democracy – study," University of Birmingham, 27 Jul. 2022

4 Feldmann, Magnus and Morgan, Glenn. "Business and Populism: The Political Economy of the 'Odd Couple'," Oxford Academic, Feb. 2023

5 Shirado, Hirokazu et al. "Collective communication and behaviour in response to uncertain 'Danger' in network experiments," The Royal Society Publishing, 27 May 2020

6 Bush, Michael. "2024 Edelman Trust Barometer Reveals Innovation has Become a New Risk Factor for Trust," PR Newswire, 14 Jan. 2024

7 Burt, Tom. "Espionage fuels global cyberattacks," Microsoft On the Issues, 5 Oct. 2023

8 "Four Threats to Critical Infrastructure," Gallagher, Sep. 2023

9 Lohrmann, Dan. "2023's Dark Horse Cyber Story: Critical Infrastructure Attacks," Government Technology, 3 Dec. 2023

10 "Significant Cyber Incidents," CSIS – Strategic Technologies Program, 2024

11 "Significant Cyber Incidents," CSIS – Strategic Technologies Program, 2024

12 "NCSC Annual Review 2023: Threats and risks," National Cyber Security Centre, 14 Nov. 2023

13 "The New Frontline of Geopolitics | Understanding the Rise of State-Sponsored Cyber Attacks," SentinelOne, 6 Aug. 2023

14 Kohen, Isaac. "Motive & Effect: Implications of the NotPetya Attack," Teramind, 19 Jul. 2017

15 Farley, John. "2024 Cyber Insurance Market Conditions Outlook," Gallagher, Jan. 2024

16 "Global Risks Report 2024," World Economic Forum, 10 Jan. 2024

17 Tsonchev, Andrew. "Digitizing the Dark: Cyber-attacks against power grids threaten modernity itself," DarkTrace, 30 Jul. 2019

18 "Understanding Cyber Threats in Transport," European Union Agency for Cybersecurity, 21 Mar. 2023

19 "Check Point Software's 2023 Cyber Security Report," Check Point, 2023

20 "Homeland Threat Assessment 2024," Homeland Security 13 Sep. 2023

21 "Homeland Threat Assessment 2024," Homeland Security 13 Sep. 2023

22 Satter, Raphael. "Microsoft: Foreign hackers are targeting Biden and Trump camps," Reuters, 11 Sep. 2020

23 Banas, Adam et al. "The Risk of a Cyber Catastrophe," Gallagher Re, 2023

24 "Cybercrime: Critical infrastructure is at risk and needs a combined private- and public-sector response," World Economic Forum, 14 Jul. 2023

25 Tisdall, Simon. "Democracy's Super Bowl: 40 elections that will shape global politics in 2024," The Guardian, 17 Dec. 2023

26 "Cybercrime: Critical infrastructure is at risk and needs a combined private- and public-sector response," World Economic Forum, 14 Jul. 2023

27 "Hunting Russian Intelligence "Snake" Malware," CISA, 9 May 2023

28 "AI: Keeping Pace With the Cybercriminals," Gallagher, Nov.2023

29 Brooks, Chuck. "Cybersecurity Trends & Statistics For 2023; What You Need To Know," Forbes, 5 Mar. 2023

30 "What is Cyber Espionage?,"VMware

31 "What is Zero Trust Security?," VMware

AJG.com **The Gallagher Way.** Since 1927.